

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)	
(Briefly describe the property to be searched)	
or identify the person by name and address))	Case No. 22-863M(NJ)
Information associated with Apple ID:)	
idtr_black@yahoo.com that is stored at a)	
premises controlled by Apple, Inc.)	

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (*identify the person or describe the property to be seized*):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before May 16, 2022 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for _____ days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 05/02/2022 2:20 pm

the later specific date of _____

Nancy Joseph

Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

ReturnCase No.:
22-863M(NJ)

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple IDs : **idtr_black@yahoo.com** (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from July 19, 2021, through May 1, 2022, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from July 19, 2021, through May 1, 2022, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks associated with the account from July 19, 2021, through May 1, 2022;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades associated with the account from July 19, 2021, through May 1, 2022;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps associated with the account from July 19, 2021, through May 1, 2022;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of state and federal controlled substances laws and money laundering laws including Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 1956 and 1957, and other related offenses involving Jonte MARSHALL, Lemonda WARD, Shomari HOOPER, Oscar RAMIREZ-RIVERA, and others since January 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: the sale of illegal drugs and the laundering of proceeds of drug sales.

The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

c. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

d. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____.

_____.

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with Apple ID:
idtr_black@yahoo.com that is stored at a premises
controlled by Apple, Inc.

Case No.22-863M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. 841(a)(1) & 846; and 18 U.S.C. Sections 1956 & 1957	Distribution and Conspiracy to Distribute a Controlled Substance; and Laundering of Monetary Instruments

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

MATTHEW COOPER (Affiliate) Digitally signed by MATTHEW COOPER (Affiliate)
Date: 2022.05.02 14:05:16 -05'00'

Applicant's signature

Matthew Cooper, DEA Task Force Officer

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone _____ (specify reliable electronic means):

Date: 5/2/22 @ 2:22pm

City and state: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS**

I, Task Force Officer Matthew Cooper, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple IDs that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am employed as a Detective with the Milwaukee Police Department and have been a law enforcement officer for over 24 years. I have been a Detective for over 18 years and have been assigned to conduct narcotics investigations for over 17 years. I was previously assigned to the Vice Control Division (Narcotics) as a Police Officer for over 2 years. I have been assigned to the High Intensity Drug Trafficking Area (HIDTA) for over 14 years. I am also a Task Force Officer with the United States Department of Justice, Drug Enforcement Administration (DEA), and have been since October, 2008. As such, I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

3. I have participated in numerous complex narcotics investigations which involved violations of state and federal controlled substances laws and money laundering laws including

Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 1956 and 1957, and other related offenses. I have had both formal training and have participated in numerous complex drug trafficking investigations, including ones using wiretaps.

More specifically, my training and experience includes the following:

- a. I have utilized informants to investigate drug trafficking. Through informant interviews, and extensive debriefings of individuals involved in drug trafficking, I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin and throughout the United States;
- b. I have also relied upon informants to obtain controlled substances from dealers, and have made undercover purchases of controlled substances;
- c. I have extensive experience conducting street surveillance of individuals engaged in drug trafficking. I have participated in the execution of numerous search warrants where controlled substances, drug paraphernalia, and drug trafficking records were seized;
- d. I am familiar with the appearance and street names of various drugs, including marijuana, heroin, cocaine, cocaine base (unless otherwise noted, all references to crack cocaine in this affidavit is cocaine base in the form of crack cocaine), ecstasy, and methamphetamine. I am familiar with the methods used by drug dealers to package and prepare controlled substances for sale. I know the street values of different quantities of the various controlled substances;
- e. I am familiar with the language utilized over the telephone to discuss drug trafficking, and know that the language is often limited, guarded, and coded;
- f. I know that drug traffickers often use electronic equipment and wireless and land line telephones to conduct drug trafficking operations;
- g. I know that drug traffickers commonly have in their possession, and at their residences and other locations where they exercise dominion and control, firearms, ammunition, and records or receipts pertaining to such;
- h. I have been assigned to court-authorized wiretaps and have been trained to operate the equipment utilized to conduct such operations;
- i. I know that drug traffickers often put their telephones in nominee names in order to distance themselves from telephones that are utilized to facilitate drug trafficking; and

j. I know that drug traffickers often use drug proceeds to purchase assets such as vehicles, property, and jewelry. I also know that drug traffickers often use nominees to purchase and/or title these assets in order to avoid scrutiny from law enforcement officials.

4. I am currently participating in an investigation of a fentanyl trafficking organization led by Jonte MARSHALL, hereinafter referred to as the MARSHALL DTO. I am familiar with the facts and circumstances regarding this investigation as a result of my personal participation in this investigation, and my review of: (a) consensually recorded telephone conversations and face-to-face meetings; (b) reports prepared by, and information obtained from, other federal, state, and local law enforcement agents and officers, all of whom I believe to be truthful and reliable; and (c) information obtained from cooperating citizen witnesses, confidential sources, and defendants, whose reliability is established herein.¹ This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence that violations of Title 21, United States Code, Sections 841(a)(1) and 846, and Title 18, United States Code, Sections 1956 and 1957, as described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

¹ Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.”

PROBABLE CAUSE

7. In April 2019, case agents met with a confidential source, hereinafter referred to as "CS-1."² CS-1 provided information regarding suspects involved in drug trafficking in the Milwaukee, Wisconsin, area. CS-1 identified Jonte MARSHALL as a large-scale distributor of heroin, cocaine, and marijuana in the Milwaukee area. CS-1 identified one of MARSHALL's phone numbers as (414) 779-1998. CS-1 identified MARSHALL's residence as a duplex at 1929 and 1931 South 97th Street, West Allis, Wisconsin. CS-1 stated this residence is a duplex owned by MARSHALL. MARSHALL lives in the lower unit of the duplex and stores drugs in the upper unit of the duplex. CS-1 stated that MARSHALL carries a pistol on his person at all times.

8. CS-1 believed that Jonte MARSHALL receives at least some of his drugs through the mail. On one occasion, CS-1 was at the residence of MARSHALL's associate, Corey Vance, when a third subject was at the residence waiting to receive a parcel believed to contain drugs. CS-1 left the residence before the parcel arrived. CS-1 stated MARSHALL owns a residence in Arizona and travels to Arizona frequently to conduct drug trafficking activities.

9. CS-1 identified another subject involved in drug trafficking with Jonte MARSHALL as Corey Vance. CS-1 stated Vance distributes large amounts of heroin, cocaine,

² Case agents believe CS-1 is a reliable person because CS-1 has provided information which law enforcement has been able to corroborate through independent investigations, CS-1 has provided statements against CS-1's own penal interests, and CS-1 has conducted controlled buys of narcotics for law enforcement. CS-1's adult criminal history includes two misdemeanor convictions and one felony conviction. CS-1 is cooperating in exchange for consideration on a pending felony arrest. Criminal charges were subsequently declined based on CS-1's cooperation. CS-1 was paid a total of \$3,000 on four separate occasions for providing information on multiple felony offenses occurring in the Milwaukee area.

and marijuana for MARSHALL. CS-1 identified Vance's residence as 5908 North 69th Street, Milwaukee, Wisconsin. CS-1 stated Vance lives at this residence with his mother. CS-1 stated that within several days of the interview CS-1 had been inside this residence and seen five different handguns. CS-1 further stated that Vance always carries a handgun in his waistband. CS-1 stated Vance also stores drugs at this residence and observed about 100 grams of heroin in the residence about two weeks earlier.

10. CS-1 stated that when CS-1 would purchase heroin from Vance and MARSHALL, a girlfriend of MARSHALL's would arrive at the residence with the heroin. Vance would leave the residence with the money, meet with the unidentified girlfriend of MARSHALL, then return to the residence with the heroin. Despite CS-1's belief that MARSHALL and VANCE distribute heroin, all of the suspected "heroin" seized to date has tested positive for fentanyl rather than heroin.

Controlled Purchases of Drugs from the Jonte MARSHALL DTO

11. On April 18, 2019, CS-1 placed a recorded and monitored call to Corey Vance. Vance answered the phone. CS-1 asked Vance about purchasing "50" the following day and asked if the transaction could take place at 11:00 a.m. or 12:00 p.m. Vance agreed and the call ended. Telephone records show that a short time later Vance called Jonte MARSHALL at (414) 779-1998. Case agents believe Vance called MARSHALL to relay CS-1's request to purchase drugs.

12. On April 19, 2019, CS-1 exchanged a series of text messages with Vance. That morning, case agents established surveillance at the residence of Jonte MARSHALL, and at the residence of Corey Vance. CS-1 was given \$3,000 in pre-recorded buy money and an audio recording and monitoring device. CS-1 received a text message from Vance which told CS-1 to come to Vance's residence to complete the transaction. At about the same time, case agents

observed Jonte MARSHALL walk from the rear of his residence. MARSHALL entered the driver's seat of a black Cadillac Escalade and backed out of the driveway. The vehicle was not followed.

13. CS-1 arrived at Vance's residence and went inside. A short time later, case agents observed MARSHALL's black Cadillac Escalade arrive and park near Vance's residence. A few minutes later, Vance exited his residence and entered the front passenger seat of the Escalade. Vance exited the Escalade about 20 seconds later and re-entered his residence. The Escalade then departed the area followed by several surveillance units.

14. A short time later, CS-1 exited Vance's residence. CS-1 was followed directly to a pre-determined meet location. Upon arrival, CS-1 turned over to case agents a clear plastic, knotted baggie containing a tan, chunky substance suspected to be fentanyl. CS-1 stated that upon entering the residence, CS-1 met with Vance and handed the pre-recorded buy money to Vance. Vance placed a call and informed the person on the other end of the phone that CS-1 was "good." CS-1 waited in the residence for about 20 minutes with Vance. CS-1 further stated that at one point Vance received a text message and exited the residence. Less than a minute later, Vance returned to the residence and went into a back bedroom. A short time later, Vance returned to the living room and handed CS-1 the baggie containing the tan, chunky substance. Vance told CS-1 he had weighed the baggie and it weighed 50 grams. CS-1 then left the residence and returned to the predetermined meet location. The suspected fentanyl later tested positive for fentanyl with a total weight of 51.62 grams.

15. Surveillance units followed the Cadillac Escalade to a local BMO Harris Bank. MARSHALL exited the Escalade and entered the bank. Case agents later obtained surveillance video from the BMO Harris Bank branch. A review of the video showed MARSHALL enter the

bank and meet with a bank teller. MARSHALL removed a large amount of United States currency from his pocket and deposited it into an unknown bank account.

16. Case agents have made ten additional controlled purchases of fentanyl from members of the Jonte MARSHALL DTO. From May 8, 2019, through September 26, 2019, CS-1 purchased an additional 450 grams of fentanyl from Corey Vance and Jonte MARSHALL. MARSHALL was in regular phone contact with Vance surrounding each of these transactions. During surveillance of several of the controlled buys, case agents observed Lemonda WARD deliver the fentanyl to Corey Vance prior to Vance delivering it to CS-1. Therefore case agents believe Lemonda WARD is a courier for the MARSHALL DTO. On October 11, 2019, Corey Vance died of natural causes. CS-1 attended a funeral service for Vance and met with Jonte MARSHALL. MARSHALL directed CS-1 to start purchasing fentanyl from Shomari HOOPER. CS-1 agreed.

17. In November 2019, CS-1 purchased approximately 50 grams of fentanyl from Shomari HOOPER at HOOPER's residence. In February 2020, CS-1 purchased approximately 50 grams of fentanyl from HOOPER at HOOPER's residence. In April 2020, CS-1 purchased approximately 100 grams of fentanyl from HOOPER at HOOPER's residence. Lemonda WARD delivered the fentanyl to HOOPER prior to HOOPER's transaction with CS-1. In June 2020, CS-1 purchased approximately 100 grams of fentanyl from HOOPER at HOOPER's residence. In November 2020, the CS purchased approximately 100 grams of fentanyl from HOOPER at HOOPER's residence. During the controlled buy, the CS observed approximately 300 grams of fentanyl in HOOPER's residence along with blenders commonly used to prepare fentanyl for distribution.

18. During each of the controlled buys from HOOPER, CS-1 was equipped with an audio monitoring device. Telephone records show that Jonte MARSHALL, using (414) 779-1998, was in contact with Shomari HOOPER and Lemonda WARD in the days surrounding each of the controlled buys. During the April controlled buy, telephone records showed that MARSHALL, using (414) 779-1998, was coordinating the meeting between HOOPER and WARD. Prior court-authorized positional information for MARSHALL's cell phone, (414) 779-1998, also showed that MARSHALL was at HOOPER's residence several hours after the February controlled buy from HOOPER. Case agents believe MARSHALL met with HOOPER to pick up the money from the controlled buy. A review of remote surveillance video from a camera installed in the alley behind HOOPER's residence also showed MARSHALL and WARD meeting with HOOPER numerous times for short durations. These meetings are consistent with the delivery of drugs or the proceeds of drug sales.

19. Telephone records have revealed that during many of these transactions, data sessions had been opened on MARSHALL's, HOOPER's, and/or WARD's phone. Case agents are aware that data sessions are opened when the user of a cellular phone is utilizing the cellular network to send or receive data, including communications sent using alternate communication platforms. There have been numerous instances of physical and electronic surveillance when Jonte MARSHALL, Shomari HOOPER, and Lemonda WARD have been observed meeting with each other and/or other suspected members of the MARSHALL DTO, but there has not been a phone call preceding these meetings. Case agents believe that MARSHALL, HOOPER, and WARD are using a communication platform to communicate with each other and with other DTO members. Case agents are further aware that Apple FaceTime is a communication platform frequently used

by drug traffickers to communicate with each other and that the use of Apple FaceTime would cause a data session to be utilized on the user's cellular phone.

20. Additionally, a review of telephone records has revealed that during the controlled purchases of fentanyl from Shomari HOOPER, many of the text messages sent from CS-1 to HOOPER did not appear in HOOPER's phone records despite case agents being with CS-1 at the time the text messages were sent. This leads case agents to believe that these messages were sent via Apple's iMessage rather than as conventional text messages. Case agents further believe that HOOPER uses iMessage to communicate with MARSHALL and WARD.

21. On March 20, 2020, a United States Postal Inspector was conducting routine parcel screening at the United States Postal Service ("USPS") Root River Post Office, located at 11015 W Oklahoma Avenue, Milwaukee, Wisconsin 53227, when the following parcel was found to be suspicious in nature: USPS Priority Mail parcel 9405503699300286995365. The parcel was approximately an 11.25" x 8.75" x 6" USPS medium flat rate Priority Mail parcel weighing approximately 5 lbs. 8 oz. The parcel's label indicated it was from "The Variety Shoppe, PO Box 315, Dawsonville GA 30534-0006." The parcel bore a typewritten label addressed to "Jonte Marshall, 1929 S 97th St, West Allis WI 53227-1430." The parcel was postmarked on March 18, 2020, in Dawsonville, Georgia 30534. The postage paid was \$15.05.

22. The sender of the parcel, The Variety Shoppe, has a website, www.varietyshoppe.com, showing a number of products they sell including digital scales, detox products, sexual stimulants, room deodorizers, and "powdered vitamins." Their homepage shows the "top selling powdered vitamin supplements" as mannitol, inositol, niacinamide, lactose, and VitaBlend. Case agents are aware mannitol, inositol, and lactose are common cutting agents added

to narcotics prior to distribution. The website further states, “*our customers receive an e-mail after the order is shipped containing an estimated time of arrival and a tracking number for the order.*”

23. A check of USPS business records showed that since June 2018 the destination address of the parcel, 1929 South 97th Street, has received at least 35 packages originating from Dawsonville, Georgia. At least 15 of these packages have all been from the same sender’s address as the parcel sent on March 18, 2020, and have all shown the same approximate weight as this parcel. The USPS business records were not kept for the remaining 20 parcels. Postal Inspectors were unable to confirm the sender’s name and address of these parcels but suspect they all originated from the Variety Shoppe due to the type of USPS shipment used, the originating Post Office, and the weight of the parcels being the same as this parcel.

24. On March 20, 2020, case agents applied for and received a federal sneak and peek search warrant for the parcel. The search warrant was issued by United States Magistrate Judge Nancy Joseph in the Eastern District of Wisconsin. Upon executing the search warrant on the parcel on March 20, 2020, case agents discovered the parcel contained two containers of Seven Stars Superior Lactose in powder form. The label for each container showed they each contained “2.2 lbs/1000 grams” of lactose. The parcel also contained a packing slip which showed the order was taken by The Variety Shoppe from Jonte MARSHALL with an email address of ldtr_black@yahoo.com.³ Case agents repackaged the parcel with all of its original contents and placed it back into the mail stream. The parcel was delivered on March 21, 2020, at approximately 10:41 a.m.

³ Case agents believe this particular order contained a typo of MARSHALL’s actual email address where the first letter, “i” was changed to an “l.”

25. On September 30, 2019, a Grand Jury subpoena was served on Apple for information related to (414) 779-1998, the cellular phone used by Jonte MARSHALL. On October 10, 2019, case agents received a response from Apple. The response identified the Apple ID associated with (414) 779-1998 as **idtr_black@yahoo.com**. The Apple response further identified Jonte MARSHALL's email address as idtr_black@yahoo.com.

26. On May 12, 2020, the Honorable William E. Duffin, United States Magistrate Judge in the Eastern District of Wisconsin, signed a warrant for information associated with the Apple ID idtr_black@yahoo.com. Case agents subsequently served that warrant on Apple. On May 29, 2020, case agents received a response from Apple. As detailed below, information received from Apple revealed that MARSHALL, using (414) 779-1998, was in regular contact with a subject later identified as Oscar RAMIREZ-RIVERA. Case agents believe, based on the investigation to date, that RAMIREZ-RIVERA was a fentanyl source of supply to MARSHALL and that MARSHALL would send money to Arizona as payment for fentanyl received from RAMIREZ-RIVERA.

27. The Apple response showed that from January 29, 2018, at 8:45 p.m.⁴, through July 12, 2019, MARSHALL, using (414) 779-1998, exchanged numerous iMessages with (602) 391-0291, an Arizona phone number. Many of these messages requested simply that one party call the other one. Both MARSHALL and the user of (602) 391-0291 referred to each other as "Mano." On February 13, 2018, at 7:55 p.m., MARSHALL, using (414) 779-1998, sent an iMessage to (602) 391-0291 that read, "Text me your full name here." On February 13, 2018, at 7:58 p.m., the

⁴ All times referenced in the Apple information are in UTC time. Milwaukee, Wisconsin is five hours behind UTC times during daylight savings hours and six hours behind UTC during standard time.

user of (602) 391-0291 sent an iMessage back to MARSHALL at (414) 779-1998 that read, “Oscar Manuel Ramirez Rivera.” On February 10, 2019, at 12:52 a.m., the user of (602) 391-0291 sent an iMessage to MARSHALL at (414) 779-1998. The iMessage contained a photograph of a State of Washington Identification Card in the name of Oscar Manuel RAMIREZ-RIVERA. The card listed an address in Yakima, Washington. On February 10, 2019, at 12:53 a.m., MARSHALL, using (414) 779-1998, sent an iMessage back to (602) 391-0291 that read, “CONGRATULATIONS U FUCKIN AMERICAN!!! Lol!!.” On February 10, 2019, at 12:54 p.m., the user of (602) 391-0291 sent an iMessage to MARSHALL at (414) 779-1998 that read, “I wish.” Case agents believe that RAMIREZ-RIVERA sent MARSHALL a photo of an identification card he had been issued. MARSHALL joked that RAMIREZ-RIVERA was now an American citizen. Case agents believe that Oscar Manuel RAMIREZ-RIVERA was the user of (602) 391-0291. The Apple responses further revealed instances dating back to 2016 of Oscar RAMIREZ-RIVERA’s name being sent by MARSHALL, using (414) 779-1998, to others with directions to send wire transfers to or make deposits into bank accounts utilized by RAMIREZ-RIVERA.

28. On April 29, 2019, at 4:28 a.m., RAMIREZ-RIVERA, using (602) 391-0291, sent an iMessage to MARSHALL at (414) 779-1998 containing a screenshot of the Cash App application. Cash App allows users to send money directly to each other without using a bank or telegram service. The screenshot contained the name “Luis Alberto Molina” and the username “\$molinalui.” Case agents believe this was a request by RAMIREZ-RIVERA for MARSHALL to send money to “Luis Alberto Molina.” On April 30, 2019, at 9:44 p.m., MARSHALL, using (414) 779-1998, sent an iMessage containing a screenshot from Cash App to RAMIREZ-RIVERA at (602) 391-0291 that contained a message that read, “Cash couldn’t be sent. This would exceed

your \$7,500/week limit.” Case agents believe MARSHALL had attempted to send money to “Luis Alberto Molina,” but the transaction was denied. On April 30, 2019, at 9:45 p.m., MARSHALL, using (414) 779-1998, sent an iMessage to RAMIREZ-RIVERA at (602) 302-0291 that read, “Maybe \$25 right now?” On April 30, 2019, at 9:48 p.m., RAMIREZ-RIVERA, using (602) 391-0291, sent an iMessage to MARSHALL at (414) 779-1998 that read, “Can you send it the old way for Friday Mano we have no more food in the fridge.” Case agents believe MARSHALL offered to send “\$25,” possibly a reference to \$2,500 and RAMIREZ-RIVERA requested the money be sent in the same manner it had previously been sent and indicated they did not have any money at the moment (“food in the fridge”). On April 30, 2019, at 9:50 p.m., MARSHALL, using (414) 779-1998, sent an iMessage to RAMIREZ-RIVERA at (602) 391-0291 that contained a screenshot from Cash App that read, “Your \$2,500 payment will be sent shortly.” On April 30, 2019, at 9:51 p.m., RAMIREZ-RIVERA, using (602) 391-0291, sent an iMessage to MARSHALL at (414) 779-1998 that read, “To which one Mano.” On April 30, 2019, at 9:54 p.m., MARSHALL, using (414) 779-1998, sent an iMessage to RAMIREZ-RIVERA at (602) 391-0291 that read, “L.” Case agents believe MARSHALL sent \$2,500 to RAMIREZ-RIVERA for drugs previously received. RAMIREZ-RIVERA asked which account MARSHALL had sent the money to and MARSHALL replied “L,” a reference to Luis Alberto Molina.

29. On July 15, 2019, at 6:15 p.m., an iMessage was sent from (602) 703-0618 to (414) 779-1998 that read, “Mano call me.” Case agents believe this was a new phone being used by Oscar Manuel RAMIREZ-RIVERA.” On December 10, 2019, at 2:36 p.m., RAMIREZ-RIVERA, using (602) 703-0618, sent an iMessage to (414) 779-1998 that contained a photo of two subjects, one of whom was Oscar RAMIREZ-RIVERA. Based on other iMessages, case agents are aware that RAMIREZ-RIVERA was arriving in Milwaukee that day. The photo appears to have been

taken at General Mitchell International Airport in Milwaukee. Case agents believe RAMIREZ-RIVERA sent a photo of himself at the airport to tell MARSHALL he had arrived in Milwaukee. On February 22, 2020, at 5:42 p.m., MARSHALL, using (414) 779-1998, sent an iMessage to RAMIREZ-RIVERA at (602) 703-0618 that read, “HAPPY BIRTHDAY MANO!!! I’ll call you in a few.” Case agents are aware that Oscar RAMIREZ-RIVERA was born on February 22, 1992. For these reasons, case agents believe that Oscar RAMIREZ-RIVERA was the user of (602) 703-0618.

30. On November 28, 2019, at 11:25 p.m., RAMIREZ-RIVERA, using (602) 703-0618, sent an iMessage to MARSHALL at (414) 779-1998 that read, “Mano you put the old ready.” On November 28, 2019, at 11:25 p.m., MARSHALL, using (414) 779-1998, sent an iMessage back to (602) 703-0618 that read, “Yup.” On November 28, 2019, at 11:26 p.m., RAMIREZ-RIVERA, using (602) 703-0618, sent an iMessage back to (414) 779-1998 that read, “Ok cool.” On November 29, 2019, at 12:12 a.m., RAMIREZ-RIVERA, using (602) 703-0618, sent an iMessage to MARSHALL at (414) 779-1998 that read, “Mano I need the name who send it.” On November 29, 2019, at 12:12 p.m., MARSHALL, using (414) 779-1998 sent an iMessage to RAMIREZ-RIVERA at (602) 703-0618 that read, “Lemonda Ward.” On November 29, 2019, at 12:12 a.m., RAMIREZ-RIVERA, using (602) 703-0618, sent an iMessage to MARSHALL at (414) 779-1998 that read, “For both.” On November 29, 2019, at 12:47 a.m., MARSHALL, using (414) 779-1998, sent two iMessages to RAMIREZ-RIVERA at (602) 703-0618 that read, “Yup” followed by “1k each.” Case agents believe RAMIREZ-RIVERA asked MARSHALL to send money to him using a prior method they used to send money (“put the old”). MARSHALL told RAMIREZ-RIVERA he had sent the money. RAMIREZ-RIVERA asked for the name of the person that sent the money and MARSHALL told him they were sent by Lemonda WARD, a

known courier for the MARSHALL DTO. RAMIREZ-RIVERA asked if that was the sender for both wires and MARSHALL said it was and that each of the wires was for \$1,000. Case agents believe this money was payment for drugs MARSHALL previously received from RAMIREZ-RIVERA.

31. On June 11, 2020, a United States Postal Inspector was reviewing United States Postal Service (“USPS”) business records when a Priority Mail parcel was found to be suspicious. The postal records indicated that a parcel had been shipped to “Jon Marshall” at 1929 South 97th Street, West Allis, Wisconsin. The Postal Inspector examined the USPS business records and open-source website information and determined that the parcel had been shipped from a company named “Kief Presses.” A review of the website for Kief Presses, <http://www.kiefpresses.com>, revealed that the company manufactured and sold four different presses, which the company described as “pollen” presses. I am aware, based on my training and experience, that presses of this type are commonly used to compress powdered narcotics, such as fentanyl, heroin, and cocaine, into compressed “bricks” after they have been diluted with cutting agents.

32. A review of postal records revealed that the parcel shipped to Jonte MARSHALL from Kief Presses was being tracked from Jonte MARSHALL’s residence at 8320 West Mourning Dove Court, Mequon, Wisconsin. An Administrative Subpoena previously served on Charter Communications revealed that the internet service at that residence was subscribed to Jonte MARSHALL with an email address of idtr_black@yahoo.com. That same day, MARSHALL was also due to receive another parcel from The Variety Shoppe, which case agents believe, based on the investigation to date, contained more lactose. That package had also been shipped to 1929 South 97th Street, West Allis, Wisconsin. Both parcels were delivered on Friday, June 12,

2020. Case agents believe that MARSHALL had purchased a press and additional quantities of a cutting agent in order to manufacture additional quantities of fentanyl, heroin, and/or cocaine, and to press those powders into “brick” form.

33. On June 19, 2020, the Honorable Stephen C. Dries, United States Magistrate Judge in the Eastern District of Wisconsin, signed a warrant for information associated with the email address idtr_black@yahoo.com that was in possession of Yahoo!. On June 30, 2020, case agents received a response from Yahoo!. The response contained over 20,000 emails sent or received by MARSHALL from January 1, 2019, through June 19, 2020.

34. Several of the emails revealed tracking updates from FedEx for parcels being sent from “John marshall, Blackout Investments LLC” on March 2, 2020; April 16, 2020; and May 19, 2020. Case agents are aware that Jonte MARSHALL is the registered agent for Blackout Investments LLC and that he frequently refers to himself as “John” in numerous emails. The March 2, 2020, parcel was sent to “Oscar Ramirez” at a FedEx Ship Center in Los Angeles, California. The parcel was delivered on March 3, 2020, and was signed for by “O. Ramirez.” The April 16, 2020, parcel was sent to Luis MATA-TORRES at 10620 W. Illini St, Tolleson, Arizona. A review of public databases and social media information revealed that Oscar RAMIREZ-RIVERA shares several addresses and appears to be romantically involved with Mirna MATA. Public databases and social media information indicate that Mirna MATA has a brother named Luis MATA-TORRES. This parcel was delivered on April 17, 2020. The May 19, 2020, parcel was also addressed to Luis MATA-TORRES at 10620 W. Illini St, Tolleson, Arizona. This parcel was delivered on May 20, 2020. Case agents believe these parcels contained payment to Oscar RAMIREZ-RIVERA for drugs previously received by MARSHALL.

35. On June 17, 2020, case agents sent an Administrative Subpoena to FedEx Express for information on parcels sent using the FedEx account of “John marshall, Blackout Investments LLC.” On July 7, 2020, case agents received records from FedEx. The records confirmed the three parcels described above. The records also indicated seven additional parcels had been sent to Luis MATA-TORRES and one parcel had been sent to Cindi MATA. All the parcels were delivered to addresses known to be associated with Mirna MATA and/or Oscar RAMIREZ-RIVERA or addresses that Oscar RAMIREZ-RIVERA had provided to Jonte MARSHALL via iMessage.

36. On July 20, 2020, the Honorable Nancy Joseph, United States Magistrate Judge in the Eastern District of Wisconsin, signed warrants authorizing the search of (414) 779-1998 and (602) 703-0618. More specifically, the warrants directed AT&T and T-Mobile to provide information about the location of (414) 779-1998 and (602) 703-0618 for a period of 45 days.

37. Case agents monitoring the location of (602) 703-0618 observed that RAMIREZ-RIVERA had been primarily in the Phoenix, Arizona area until July 31, 2020. On July 31, 2020, RAMIREZ-RIVERA travelled from Phoenix to Los Angeles, California. From July 31, 2020, until August 5, 2020, RAMIREZ-RIVERA remained in California and frequented the areas of Palmdale, California; Llano, California; and San Bernardino, California. On August 5, 2020, RAMIREZ-RIVERA returned to the Phoenix area. On Thursday, August 6, 2020, at 10:20 p.m., court-authorized positional information for (602) 703-0618 indicated that RAMIREZ-RIVERA was at the airport in Milwaukee, Wisconsin. RAMIREZ-RIVERA remained in the Milwaukee area and his phone was frequently observed at the same locations as MARSHALL's cellular phone.

38. On August 12, 2020, at 8:50 a.m., court-authorized positional information for (602) 703-0618 indicated that RAMIREZ-RIVERA's cellular phone was in close proximity to 7836

North Faulkner Road, Milwaukee, Wisconsin. This is the location of Schweiger and Baumann Trucking LLC, a business owned by Jonte MARSHALL. At 9:01 a.m., court-authorized positional information for (414) 779-1998, MARSHALL's cellular phone, indicated MARSHALL was also in that area. At 9:20 a.m. and 9:35 a.m., (602) 703-0618 was located in close proximity to MARSHALL's residence at 8320 West Mourning Dove Court, Mequon, Wisconsin. At 9:18 a.m. and 9:36 a.m., (414) 779-1998 remained near 7836 North Faulkner Road. At 9:50 a.m., (602) 703-0618 was again in the area of 7836 North Faulkner Road. At 10:05 a.m., (602) 703-0618 was located in the area of North 76th Street and West Brown Deer Road which is between MARSHALL's residence and 7836 North Faulkner Road. At 10:07 a.m., (414) 779-1998 was located near MARSHALL's residence. At 10:20 a.m., (602) 703-0618 was located near North 76th Street and West Bradley Road which is approximately 13 blocks east of 7836 North Faulkner Road.

39. At 10:25 a.m., case agents began to conduct surveillance at 7836 North Faulkner Road, Milwaukee, Wisconsin. At 10:25 a.m., case agents observed Jonte MARSHALL's black 2018 Cadillac Escalade, bearing Wisconsin license plates AGE-4015, parked in the southeast corner of the rear parking lot at that location. These license plates list to Blackout Investments LLC at 7836 North Faulkner Road, Milwaukee, Wisconsin. Jonte MARSHALL is the registered agent for Blackout Investments LLC. Case agents also observed Jonte MARSHALL standing in the rear parking lot at that location. MARSHALL appeared to be taking a picture of a vehicle in a rear parking area. The vehicle could not be seen as it was parked between other large vehicles. Court-authorized positional information also confirmed that (414) 779-1998 was at that location at 10:25 a.m. Case agents established surveillance where they could observe vehicles coming and going from the business, but could not observe most of the rear parking lot.

40. At 10:35 a.m., court-authorized positional information for (602) 703-0618 indicated it was located near 7836 North Faulkner Road. At 10:39 a.m., case agents observed a gray 2016 Jeep Grand Cherokee, bearing California license plates 8ADB961, drive from the rear parking lot and turn south on North Faulkner Road. These license plates list to Carlos ESTRADA at 13841 Beech Street, Victorville, California 92392. This vehicle was not followed. At 10:41 a.m., (414) 779-1998 was still located near 7836 North Faulkner Road. At 10:48 a.m., case agents observed Jonte MARSHALL walk across the rear parking lot and enter the driver's seat of his Cadillac Escalade. MARSHALL drove the Escalade out of the parking lot and turned north on North Faulkner Road. Case agents attempted to locate MARSHALL's vehicle, but were unsuccessful.

41. At 10:49 a.m., court-authorized positional information for (602) 703-0618 indicated it was located near 7300 West Good Hope Road, Milwaukee, Wisconsin. Case agents went to that location in an attempt to locate RAMIREZ-RIVERA. At 10:58 a.m., case agents observed a commercial car carrier in the parking lot at approximately 7208 North 76th Street, Milwaukee, Wisconsin. Case agents observed a gray Jeep Grand Cherokee on the upper cargo area of the car carrier and confirmed that the license plate on the Jeep was the same license plate of the Jeep observed leaving 7836 North Faulkner Road. Case agents were unable to locate RAMIREZ-RIVERA at that location and then began to conduct surveillance of the car carrier and Jeep.

42. Case agents maintained surveillance of the car carrier until it entered Interstate 94 eastbound toward Chicago, Illinois. The car carrier was followed into Racine County, Wisconsin. At 12:34 p.m., a Wisconsin State Patrol Inspector conducted a traffic stop of the car carrier for a safety inspection. After the initial traffic stop, the car carrier was relocated to the Racine Safety

Weight Enforcement Facility for an inspection. The driver of the car carrier stated he had picked up all three of the vehicles on the car carrier from private parties in the Milwaukee area. The driver had shipping information on his phone which indicated the Jeep Grand Cherokee was being transported to Hesperia, California. The Inspector asked the driver to off-load the Jeep and one other vehicle so he could confirm the VIN numbers on each vehicle. The driver agreed to do so. A Wisconsin State Patrol Trooper then arrived on scene to assist the Inspector. The Trooper deployed his K-9 partner around the Jeep and the other vehicle and the K-9 alerted to the odor of controlled substances emanating from the Jeep. During a search of the Jeep, the Inspector and Trooper located an electronically-controlled compartment behind the rear passenger seat. The compartment was observed to contain rubber-banded United States currency. The Inspector and Trooper dismantled the compartment and removed a large amount of United States currency. An official count later revealed that \$508,140 in United States currency was located in the compartment.

43. On August 12, 2020, the DEA Detroit Field Division contacted Milwaukee case agents regarding a telephone deconfliction. The Detroit agents had received information from a source of information (SOI) related to the seizure of the currency from the Jeep Cherokee in Wisconsin and a possible future shipment of currency from Milwaukee. The SOI provided Detroit agents with specific information that Jonte MARSHALL and Oscar RAMIREZ-RIVERA planned to ship a second vehicle from Milwaukee on August 13, 2020. The SOI provided agents with the vehicle pickup location and a description of the vehicle.

44. On August 13, 2020, Milwaukee case agents established surveillance at the vehicle pickup location, the same business owned by MARSHALL, located at 7836 North Faulkner Road, Milwaukee, Wisconsin. At 8:36 a.m., case agents observed a white Ford Expedition parked in the

rear of the building. At 12:39 p.m., case agents observed the black Cadillac Escalade, bearing Wisconsin license plate AGE-3015, driven by MARSHALL, arrive at the business and park in the rear. At 12:41 p.m., court-authorized positional information for (414) 779-1998 revealed that the phone was in close proximity to 7836 North Faulkner Road, Milwaukee, Wisconsin. At 12:46 p.m., MARSHALL left the business northbound in the black Escalade. At 2:17 p.m., case agents observed a grey GMC Acadia, bearing Minnesota license plates DGA140, driven by a Hispanic male later identified as RAMIREZ-RIVERA arrive at the business and park in the rear. These license plates list to PV Holding Corporation, 2240 Airport Lane, Minneapolis, Minnesota 55450. PV Holding Corporation is a holding company for Avis and Budget rental cars. At 2:19 p.m., court-authorized positional information for (602) 703-0618 revealed that the phone was in close proximity to 7836 North Faulkner Road, Milwaukee, Wisconsin.

45. At 5:41 p.m., case agents observed a commercial car carrier arrive at the business and park in front on North Faulkner Road. The company name "Gigi Line" was printed on the side of the truck. Shortly thereafter, RAMIREZ-RIVERA drove a white 2005 Ford Expedition, bearing Wisconsin license plates AFH-7134, from the rear of the business and turned the vehicle over to the driver of the car carrier. These license plates list to Jonte MARSHALL at 1929 South 97th Street, West Allis, Wisconsin. This vehicle matched the description of the vehicle previously provided by the Detroit SOI. The driver loaded the Ford Expedition onto the car carrier while RAMIREZ-RIVERA watched.

46. Agents conducted surveillance of the car carrier for approximately three hours as it picked up additional cars in West Bend, Wisconsin. After leaving that area, case agents followed the car carrier until it entered Interstate 94 toward Chicago, Illinois. At 9:43 p.m., as the car carrier was in Racine, County, Wisconsin, a traffic stop was conducted by the Wisconsin State Patrol.

During the traffic stop and inspection, a Racine County Sheriff Deputy deployed his K-9, which gave a positive alert to the odor of controlled substances in the Ford Expedition. During a search of the vehicle, case agents located a large amount of US Currency concealed in a natural void in the driver's side rear quarter panel. An official count later determined that \$100,020 had been seized from the vehicle.

47. On September 21, 2020, the Honorable Stephen C. Dries, United States Magistrate Judge in the Eastern District of Wisconsin, signed a warrant for information associated with the email address idtr_black@yahoo.com that was in possession of Yahoo!. On October 7, 2020, case agents received a response from Yahoo!. The response contained over 10,000 emails sent or received by MARSHALL from June 19, 2020, through September 21, 2020.

48. A review of emails sent to and from idtr_black@yahoo.com revealed that Jonte MARSHALL continued to utilize this email address to further the drug trafficking and money laundering activities of the MARSHALL DTO. For example, on June 20, 2020, an email was sent from eBay (ebay@ebay.com) to idtr_black@yahoo.com that confirmed delivery of “1 Kilogram – Top Grade Superior Lactose Powder.” As detailed above, case agents believe that the MARSHALL DTO utilizes lactose as a cutting agent for fentanyl. Additionally, on September 18, 2020, MARSHALL, using idtr_black@yahoo.com sent an email to tracy.bonin@rrins.com. The email contained an attachment which consisted of an appraisal, dated September 17, 2020, from Harry C. Glinberg Jewelers. The appraisal showed that MARSHALL owned a men’s Rolex watch valued at \$25,000. Case agents believe this watch was proceeds of MARSHALL’s drug trafficking and that he sought to have the watch insured.

49. On September 18, 2020, an email was sent from mgcnewspaper@yahoo.com to idtr_black@yahoo.com and to “Navroze” at navrozelalani@yahoo.com. The email contained an

attachment entitled “Letter of Intent Agreement.” The contents of the agreement show that Jonte MARSHALL intended to purchase a business known as Express Liquor from Mr. Ali Navroze.⁵ The agreement is not fully completed and was not signed. Case agents subsequently learned from CS-1 that Jonte MARSHALL did purchase Express Liquor at 3833 North Teutonia Avenue, Milwaukee, Wisconsin, and that MARSHALL utilizes the business to launder the proceeds of drug trafficking.

50. Additionally, in November 2020, case agents were contacted by Department of Homeland Security – Homeland Security Investigation (HSI) Agents in Dallas, Texas based on a phone deconfliction. HSI Agents had conducted a money pickup of \$150,000 from Navroze LALANI. LALANI informed an HSI confidential source that he was laundering the money for someone in Milwaukee, Wisconsin and that the Milwaukee-based subjects had an additional \$500,000 to launder. LALANI is in regular and frequent contact with Jonte MARSHALL, as recently as June 29, 2021. Case agents believe LALANI is assisting in the laundering of drug proceeds for the MARSHALL DTO.

51. On December 21, 2020, a search warrant was executed at 326 West Florida Street #403, Milwaukee, Wisconsin. The target of this warrant was Jovan NEWMAN. Case agents are aware, based the investigation to date, that Jovan NEWMAN is a rapper who uses the stage name of Looney Baby. Jovan NEWMAN’s brother, Barry NEWMAN, is also a rapper who uses the stage name Gwapo Chapo. Jovan NEWMAN and Barry NEWMAN have signed contracts with Blackout Entertainment MKE. The investigation to date has revealed that Jonte MARSHALL operates Blackout Entertainment MKE.

⁵ Case agents believe Navroze Lalani and Ali Navroze are the same person whose full name is Navroze Ali Lalani.

52. During the execution of the search warrant, Jovan NEWMAN was located in the residence and was taken into custody. A search of the residence revealed 131.90 grams of fentanyl, 18.20 grams of marijuana, five firearms, including a full-automatic Glock handgun, \$56,719 in United States currency, and assorted jewelry. Case agents also located numerous bottles of Seven Stars Superior Lactose in powder form, the same brand of lactose purchased from The Variety Shoppe by Jonte MARSHALL, and a large metal press within the residence. As described above, lactose is a common cutting agent used to prepare controlled substances for distribution and presses of the kind located at the residence are commonly used to compress controlled substances into hardened shapes prior to distribution. Additionally, a United States Postal Service box was located in the bedroom. This box held several additional bottles of Seven Stars Superior Lactose in powder form. The address label on this box showed that it had been shipped The Variety Shoppe in Henderson, Nevada⁶ to Christopher HILL in Milwaukee, Wisconsin. Christopher HILL is known to be a DJ who is used to promote the rap songs of Jovan NEWMAN and Barry NEWMAN. Telephone records reveal that MARSHALL, using (414) 779-1998 is in regular and frequent phone contact with Christophe HILL and Jovan NEWMAN. Case agents believe that Jovan NEWMAN and Christopher HILL assist with the manufacture and distribution of fentanyl for the MARSHALL DTO.

53. In December 2020, CS-1 informed case agents that Jonte MARSHALL planned to travel to Cancun, Mexico to meet with a new heroin source of supply. Court-authorized positional

⁶ Case agents believe that at some point during 2020, The Variety Shoppe moved from Dawsonville, Georgia to Henderson, Nevada.

information for MARSHALL's cellular phone revealed that MARSHALL did not travel to Mexico at that time.

54. On April 29, 2021, the Honorable William Duffin, United States Magistrate Judge in the Eastern District of Wisconsin, signed a warrant authorizing the renewed search of the AT&T cellular telephone assigned cellular phone number (414) 779-1998. More specifically, the warrant directed AT&T to provide information about the location of (414) 779-1998 for a period of 45 days. The Court's Order was sent to AT&T on April 29, 2021. The monitoring of the location of (414) 779-1998 began again on April 29, 2021, at 7:25 p.m.

55. Once case agents started to receive location information for (414) 779-1998, they observed that the phone was unable to be located. This generally occurs if the phone is powered off or is out of the service area of the phone provider. On May 3, 2021, case agents contacted a Department of Homeland Security - Homeland Security Investigations (DHS-HSI) Special Agent regarding any potential foreign travel of Jonte MARSHALL. The Agent consulted DHS-HSI systems and observed that MARSHALL had flown from Atlanta, Georgia to Cancun, Mexico on April 29, 2021, on Delta Airlines Flight 598. Additionally, MARSHALL was scheduled to return from Cancun to Atlanta later on May 3, 2021 on Delta Airlines Flight 1962. Court-authorized positional information for (414) 779-1998 showed that MARSHALL arrived in Atlanta on May 3, 2021, at 6:47 p.m. and then arrived in Milwaukee, Wisconsin on May 4, 2021, at 12:57 a.m.

56. On May 6, 2021, CS-1 spoke to Shomari HOOPER regarding the purchase of heroin.⁷ This call was not recorded as case agents were not with CS-1 at the time of the call. CS-1 told HOOPER that CS-1 was trying to purchase heroin from HOOPER. HOOPER replied,

⁷ As detailed above, all "heroin" purchased to date in this investigation has tested positive only for fentanyl.

"Black's gone." Case agents are aware, based on the investigation to date, that "Black" is the nickname of Jonte MARSHALL. HOOPER told CS-1 that MARSHALL was in Puerto Rico and that HOOPER was also going to Puerto Rico the following morning. HOOPER told CS-1 he planned to return to Milwaukee the following Monday or Tuesday and would talk to CS-1 about the purchase of heroin when he returned.

57. Court-authorized positional information for (414) 779-1998 showed that on May 6, 2021, at 8:26 a.m., MARSHALL was in close proximity to General Mitchell International Airport in Milwaukee, Wisconsin. A short time later the phone was powered off. At 10:46 a.m., phone location information showed the phone was in close proximity to Charlotte Douglas International Airport in Charlotte, North Carolina. A short time later, the phone powered off again. On May 6, 2021, at 3:58 p.m., court-authorized positional information for (414) 779-1998 showed that the phone was at Luis Munoz Marin International Airport in San Juan, Puerto Rico. MARSHALL remained in Puerto Rico until May 10, 2021. Phone location information showed that on May 10, 2021, the phone was at the airport in San Juan at 1:59 p.m., in Charlotte at 5:52 p.m., and in Milwaukee at 11:28 p.m. Case agents believe, based on the information provided by CS-1, the travel to Mexico by Jonte MARSHALL, followed by the subsequent travel of MARSHALL and Shomari HOOPER to Puerto Rico, that the purpose of these travels was to further the drug trafficking and money laundering activities of the MARSHALL DTO.

58. On May 28, 2021, the Honorable Stephen Dries, United States Magistrate Judge in the Eastern District of Wisconsin, signed a warrant for information associated with the Apple ID idtr_black@yahoo.com. Case agents subsequently served that warrant on Apple. On June 10, 2021, case agents received a response from Apple.

59. A review of information received from Apple pursuant to the Court's May 28, 2021 search warrant revealed that MARSHALL continues to participate in coded text message and iMessage conversations related to suspected drug trafficking. For example, on April 30, 2021, Dejuan WILEY, using (414) 719-8428, sent nine text messages to MARSHALL at (414) 779-1998. Case agents have identified Dejuan WILEY, a.k.a. "Skeet," as a pill trafficker and suspected fentanyl trafficker for the MARSHALL DTO. In these messages, WILEY was trying to get MARSHALL to call him or reply to the text message. On April 30, 2021, at 4:32 p.m., WILEY sent a message to MARSHALL that read, "Bro I gotta go so just hit me." At 7:41 p.m., MARSHALL sent a message back to WILEY that read, "My Battery went dead blood." Telephone records show that at 7:53 p.m., WILEY called MARSHALL. At 8:02 p.m., WILEY again called MARSHALL. At 8:31 p.m., MARSHALL sent a message to Lemonda WARD that read, "Wya? Need u to get something from Skeet." As detailed above, Lemonda WARD has been identified as a courier for the MARSHALL DTO. Case agents believe MARSHALL asked where WARD was and stated he needed her to pick something up from WILEY. MARSHALL and WARD then exchanged a series of messages about her location. At 8:34 p.m., MARSHALL sent a message to WARD that read, "Can you hold this bag for me from Skeet till I get back?" WARD agreed. At 8:34 p.m. and 8:35 p.m., MARSHALL sent four messages to WARD that read, "It was for Rob but he hasn't called me yet," "& this Nigga skeet cryin," "I can have him come to yo house," and "He can put it in yo car." Case agents believe WILEY called MARSHALL regarding an amount of fentanyl that was supposed to be delivered to "Rob," believed to be Robin SHRODER, a mechanic who works for MARSHALL and is suspected of being a distributor for the MARSHALL DTO. Case agents believe WILEY did not want the fentanyl at his residence and asked MARSHALL to have WARD pick it up. MARSHALL contacted WARD and asked her to pick it

up from WILEY and WARD agreed. Case agents believe additional messages between MARSHALL, WARD, and WILEY showed that WARD met with WILEY the next day to pick up the suspected fentanyl.

60. On May 1, 2021, at 10:16 p.m., MARSHALL, using (414) 779-1998, received an incoming message from (414) 698-7936, a phone believed to be used by Donta DAVIS, which read, "I fuck up lol ima need u wen u get back lol." At 10:24 p.m., MARSHALL sent a message back to DAVIS that read, "Skeet can help u 2 if it's an emergency." At 10:25 p.m., DAVIS sent a message back to MARSHALL that read, "Lol I no but if I lose it's ok but maybe yo chump ass can fix it., nope,. He cool an all but nobody coming to my crib but u or cocky lol." Case agents are aware that MARSHALL was in Mexico at the time of these messages. Case agents believe that DAVIS told MARSHALL he would need to meet with MARSHALL to obtain more fentanyl when MARSHALL returned from Mexico. MARSHALL told DAVIS that DAVIS could meet with "Skeet" to obtain fentanyl if it was an emergency. As detailed above, case agents identified "Skeet" as Dejuan WILEY. DAVIS told MARSHALL he preferred to wait for MARSHALL and that he didn't want anyone other than MARSHALL or another subject coming to his house.

61. On May 11, 2021, at 10:53 a.m., MARSHALL, using (414) 779-1998, sent a message to (414) 530-2322, a phone believed to be used by Justin JACKSON, that read, "Bring that down for me bro." JACKSON is believed to be a fentanyl distributor for the MARSHALL DTO. At 10:54 a.m., JACKSON sent a message back to MARSHALL that read, "Were." At 10:54 a.m., MARSHALL sent a message to JACKSON that read, "I'm in traffic just hit me." At 11:39 a.m., JACKSON sent a message to MARSHALL that read, "Here Macy." At 11:39 a.m., MARSHALL sent a message back to JACKSON that read, "Front or back." At 11:39 a.m., JACKSON sent a message back to MARSHALL that read, "Front." Case agents believe that

MARSHALL asked JACKSON to bring him money as payment for fentanyl previously received by JACKSON. JACKSON asked where MARSHALL wanted to meet. MARSHALL said he was driving and told JACKSON to tell him where to meet. JACKSON then told MARSHALL he was parked in front of “Macy,” believed to be the Macy’s department store located at Mayfair Mall in Wauwatosa, Wisconsin. Court-authorized positional information for (414) 779-1998 showed that at 11:37 a.m. the phone was located near North 124th Street and West Capitol Drive in Wauwatosa. At 11:52 a.m., the phone was located near North Mayfair Road and West Watertown Plank Road in Wauwatosa. Mayfair Mall is between these locations. Case agents believe MARSHALL met with JACKSON and picked up a quantity of money as payment for fentanyl previously supplied to JACKSON.

62. On May 15, 2021, at 6:39 p.m., MARSHALL, using (414) 779-1998, sent a message to (414) 998-4170, a number believed to be used by Gregory RENFRO, a suspected fentanyl distributor for the MARSHALL DTO that read, “U done?” At 6:39 p.m., RENFRO sent two messages back to MARSHALL that read, “Now i am” and “Wya.” At 6:44 p.m., MARSHALL sent a message to RENFRO that read, “Not available.” At 6:45 p.m. and 6:51 p.m., RENFRO sent two messages to MARSHALL that read, “Cash app I guess” and “Sent.” Case agents believe MARSHALL asked RENFRO if he had finished selling an amount of fentanyl previously provided to RENFRO on consignment. RENFRO stated he just finished and asked where MARSHALL was located. When MARSHALL said he was not available, RENFRO said he would send MARSHALL payment via Cash App, a mobile payment service. Other messages between MARSHALL and RENFRO indicated that RENFRO sent MARSHALL money via Cash App. Case agents believe this money was payment for fentanyl RENFRO previously received on consignment from MARSHALL.

63. On June 13, 2021, at 10:27 p.m., a Kansas Highway Patrol Trooper was monitoring traffic on US Highway 54 in Seward County, Kansas. The Trooper observed a 2022 Kenworth Semi Tractor, bearing Illinois license plate P1048444, towing a 2020 Sun Valley Car Carrier trailer, bearing Illinois license plate 717079ST, eastbound on US Highway 54. The Trooper conducted a traffic stop of the car hauler for a commercial vehicle inspection. Upon inspecting the vehicles on the car carrier, the Trooper located a white 2013 Nissan Cube that had been shipped from California and was destined for Milwaukee, Wisconsin. A subsequent search of the Nissan Cube revealed electronically controlled compartments beneath both of the vehicle's front floorboards. These compartments were found to contain 16 kilogram-shaped packages of a substance that tested positive for fentanyl and 14 packages of a substance that tested positive for cocaine. Case agents believe this fentanyl and cocaine were being transported to Milwaukee, Wisconsin to be distributed in the Eastern District of Wisconsin. Case agents removed the narcotics from the vehicle and arranged for the vehicle to be transported to Wisconsin.

64. On June 14, 2021, the Honorable Nancy Joseph, United States Magistrate Judge in the Eastern District of Wisconsin, signed a search warrant authorizing the search of the AT&T cellular phone assigned phone number (213) 379-2357. This phone had been utilized to arrange the shipment of the Nissan Cube. On June 16, 2021, at 7:45 a.m., court-authorized positional information for (213) 379-2357 showed that the phone was in close proximity to The Chalet Motel of Mequon at 10401 North Port Washington Road, Mequon, Wisconsin. Case agents responded to that location and observed a black 2016 Nissan Juke, bearing California license plates 8ROZ059.

65. On June 16, 2021, case agents met with the driver of the commercial car carrier in the Eastern District of Wisconsin. The concealed compartments in the Nissan Cube were filled

with facsimile kilogram-shaped packages similar to those seized in Kansas. The Nissan Cube was equipped with tracking devices and an alarm which would alert case agents when the concealed compartments were opened. Case agents then conducted a controlled delivery of the Nissan Cube to its delivery destination.

66. After the car carrier arrived at the delivery location, the driver contacted (213) 379-2357 via text message and advised that the vehicle had arrived. The user of (213) 379-2357 stated his “friend” would arrive shortly. Case agents observed three Hispanic males walk across the Chalet Motel parking lot and enter the Nissan Juke. These subjects were later identified as Daniel RODRIGUEZ-LARA, Richard CHAVEZ, and Humberto CORONEL-VEGA. The Nissan Juke, driven by CHAVEZ, was followed from the motel and eventually arrived at the delivery location. Daniel RODRIGUEZ-LARA exited the Nissan Juke and received the Nissan Cube from the truck driver. RODRIGUEZ-LARA drove to a nearby Walmart and parked the Cube in the parking lot. He then entered the Nissan Juke and the vehicle drove out of the area.

67. Case agents maintained surveillance of the Nissan Juke, CHAVEZ, RODRIGUEZ-LARA, and CORONEL-VEGA, for approximately six hours at which time case agents lost sight of the vehicle and surveillance was terminated. Case agents maintained constant visual surveillance of the Nissan Cube and no one returned to the vehicle. On June 16, 2021, at approximately 10:15 p.m., case agents maintaining surveillance of the Nissan Cube at Walmart observed a Yellow Cab taxi pull into the parking lot and stop near the Cube. RODRIGUEZ-LARA exited the taxi and entered the driver’s seat of the Cube. Case agents followed the Cube to Rick’s Car Care, 6121 West Mequon Road, Mequon, Wisconsin. RODRIGUEZ-LARA parked the vehicle in the parking lot and re-entered the same taxi, which had also arrived at the location. The taxi was followed to the Days Inn & Suites, 1840 North 6th Street, Milwaukee, Wisconsin.

RODRIGUEZ-LARA exited the taxi and entered the hotel. Approximately 10 minutes later, RODRIGUEZ-LARA exited the hotel with CORONEL-VEGA. They walked around the neighborhood for approximately 15 minutes before returning to the hotel. Surveillance video later showed RODRIGUEZ-LARA and CORONEL-VEGA depart the hotel on June 17, 2021, at 12:12 a.m.

68. At approximately 12:50 a.m., case agents observed a 2006 Range Rover, bearing California license plates 6NNH477, enter the parking lot of Rick's Car Care. Case agents observed two subjects enter the Nissan Cube and drive the vehicle out of the area. The vehicle was followed to North River Road south of Mequon Road where it pulled to the side of the road. Case agents received an alert that the concealed compartments inside the Cube had been opened. Case agents attempted to conduct a traffic stop of the Cube at which time the vehicle struck a law enforcement vehicle and fled at a high rate of speed. Eventually, the Cube crashed at the intersection of West County Line Road and North Wakefield Court, Bayside, Wisconsin. Both occupants of the vehicle fled and evaded capture. Case agents believe, based on the investigation to date, that CORONEL-VEGA was the driver of the Cube and Daniel RODRIGUEZ-LARA was the front passenger. A search of the vehicle revealed a pillow case on the floor of the backseat which contained 14 of the facsimile kilogram-shaped packages that were previously hidden in the concealed compartment underneath the front passenger seat. Case agents subsequently arrested Richard CHAVEZ and Daniel RODRIGUEZ-LARA.

69. On June 17, 2021, Daniel RODRIGUEZ-LARA and Richard CHAVEZ were charged by criminal complaint in the Eastern District of Wisconsin with Conspiracy to Distribute Controlled Substances and Attempted Possession with the Intent to Distribute 5 kilograms of cocaine and 5 kilograms of fentanyl. On June 22, 2021, a Grand Jury in the Eastern District of

Wisconsin returned a true bill charging RODRIGUEZ-LARA and CHAVEZ with Conspiracy to Distribute Controlled Substances and Attempted Possession with the Intent to Distribute 5 kilograms or more of cocaine and 400 grams or more of fentanyl. CORONEL-VEGA continues to be sought.

70. On June 29, 2021, case agents interviewed Richard CHAVEZ pursuant to a proffer letter. CHAVEZ stated that he was involved in the shipment of the Nissan Cube from California to Wisconsin. CHAVEZ further stated that RODRIGUEZ-LARA and CORONEL-VEGA also travelled from California to Wisconsin to assist in the delivery of the Nissan Cube. CHAVEZ stated the fentanyl and cocaine in the vehicle were destined for a subject CHAVEZ knows as “Jon” who lives in Mequon, Wisconsin. CHAVEZ described “Jon” as an African-American male 45-50 years old. CHAVEZ identified a photo of Jonte MARSHALL as the subject CHAVEZ knows as “Jon.” CHAVEZ also described the location of MARSHALL’s residence and pointed out the location on a map. The location identified by CHAVEZ was 8320 West Mourning Dove Court, Mequon, Wisconsin. Case agents are aware this is the residence of Jonte MARSHALL. CHAVEZ stated that within the last year he had arranged the delivery of over 100 kilograms of fentanyl from California to Jonte MARSHALL in Wisconsin. CHAVEZ further stated that MARSHALL had shipped in excess of \$3,000,000 in bulk United States currency from Wisconsin to California in the last year as payment for fentanyl received by the MARSHALL DTO.

71. On August 6, 2021, the Honorable Stephen Dries, United States Magistrate Judge in the Eastern District of Wisconsin, signed a warrant for information associated with the Apple ID idtr_black@yahoo.com. Case agents subsequently served that warrant on Apple. On August 11, 2021, case agents received a response from Apple. This response failed to include messages

backed up to iCloud due to a technical error. Apple eventually solved this error and provided the requested information on January 27, 2022.

72. A review of the information received from Apple indicated that MARSHALL continues to use Apple iMessage to communicate with others regarding drug trafficking and money laundering activities of the MARSHALL DTO. For example, from June 7, 2021, through June 28, 2021, MARSHALL, using (414) 779-1998, exchanged a series of iMessages with (224) 500-4039, a number used by Navroze LALANI. As detailed above, LALANI is involved in money laundering and reportedly had money available for laundering in the Milwaukee area. Additionally, as detailed above, LALANI is involved in the sale of Express Liquor in Milwaukee to MARSHALL and CS-1 previously reported that Jonte MARSHALL did purchase Express Liquor at 3833 North Teutonia Avenue, Milwaukee, Wisconsin, and that MARSHALL utilizes the business to launder the proceeds of drug trafficking. The imessages sent between June 7, 2021 and June 28, 2021, reference the ongoing purchase transaction for Express Liquor between MARSHALL and LALANI. Based on the investigation to date, case agents continue to believe that MARSHALL uses Express Liquor to launder proceeds of drug trafficking.

73. Apple iMessages received pursuant to the August 6, 2021, search warrant also demonstrate that MARSHALL continues to use (414) 779-1998 to participate in drug-related conversations. For example, on April 28, 2021, MARSHALL engages in a group message with (414) 659-4220 and (414) 676-9222, phones used by unknown subjects. In this conversation, MARSHALL arranges for his “Assistant Mel” to purchase what is believed to be ½ ounce of marijuana from MARSHALL’s associated “Mike.” The warrant also revealed numerous iMessages between MARSHALL, using (414) 779-1998, and Dejuan WILEY. Previously intercepted iMessages identified WILEY as a distributor of prescription medications and a close

associate of MARSHALL. The iMessages show numerous meetings between MARSHALL and WILEY for purposes which are not fully described, but often involve MARSHALL or WILEY meeting outside residence or in garages. MARSHALL has also directed WILEY to leave items in vehicles or at other residences for MARSHALL to pick up at a future time or to meet with Lamonda WARD, a known courier for the MARSHALL DTO. Based on the investigation to date, case agents believe these meetings involve MARSHALL and WILEY exchanging narcotics or proceeds of narcotic sales.

74. On December 20, 2021, case agents met with a confidential source who provided information regarding drug trafficking activities in the Milwaukee area. This source identified “Black” as a heroin distributor in the Milwaukee area. The source viewed a photo of Jonte MARSHALL and identified MARSHALL as the person the source knows as “Black.” The source stated MARSHALL is supplied heroin by a Mexican source of supply. The source stated that MARSHALL used to supply Jovan NEWMAN with heroin before NEWMAN’s arrest. The source stated that NEWMAN was distributing $\frac{1}{4}$ kilogram and $\frac{1}{2}$ kilogram quantities of heroin in the Milwaukee area at the time. The source further stated that MARSHALL bailed Jovan NEWMAN’s brother, Barry NEWMAN, out of jail after his arrest and that Barry NEWMAN is a rapper who works with MARSHALL’s record label, BlackOut Entertainment. The source described MARSHALL’s vehicles as a white Mercedes G-series SUV, a black Cadillac Escalade, and a black Corvette and stated MARSHALL also owns dump trucks and several investment properties. The source described MARSHALL as a major distributor of heroin in the Milwaukee area.

75. On February 24, 2022, the Milwaukee Police Department received an anonymous tip from an online tip submission form. The tip read, “large drug and gun activity going on with

TERRELL NEWMAN AND JONTE MARSHALL , SHANEQUA M JACKSON. multiple rental apartments, car rentals out of avis downtown milwaukee. driving from milwaukee to chicago for pick up that comes out of california and az. multiple businesses including liquor store, online boutique, . jonte marshall resides in mequon , terrell newman and shanaqua jackson live together at multiple locations 130 s 75th st, 655 E Norwich St, and an unknown location of a rental.”

76. A review of DEA reports revealed that MARSHALL was interviewed at the Los Angeles International Airport on February 12, 2018. During that interview, MARSHALL stated he had approximately \$12,000 in his checked bag. MARSHALL gave consent for law enforcement to search his bag where they located \$14,845 concealed within clothing. Travelling with MARSHALL was Terrell NEWMAN. NEWMAN was also interviewed. NEWMAN claimed to have approximately \$15,000 in his carry-on bag. A consensual search of the bag revealed \$43,530 concealed in a cologne box. Neither MARSHALL nor NEWMAN had a legitimate explanation for the currency and gave conflicting statements about their travel plans and reasons for being in Los Angeles. A narcotics detecting canine alerted to the presence of the scent of narcotics on the currency recovered from both MARSHALL and NEWMAN and both amounts of currency were seized by law enforcement. A review of telephone records revealed that MARSHALL, using Target Cell Phone A, continues to be in regular and frequent phone contact with (920) 371-5252, the number known to be used by Terrell NEWMAN.

77. On March 8, 2022, case agents utilized the court-authorized positional information for Target Cell Phone A to conduct physical surveillance of MARSHALL. Location information indicated the phone was in downtown Milwaukee. At 2:44 p.m., case agents located MARSHALL’s white 2021 Cadillac Escalade parked in the 1000 block of North Water Street. The vehicle was running and appeared to be occupied. Due to heavily tinted windows, case agents

were unable to confirm that MARSHALL was the driver or if there were other occupants. At 2:57 p.m., the Escalade drove away and case agents maintained surveillance of the vehicle. Due to a lack of other vehicle traffic, as the vehicle travelled west on West McKinley Street, a case agent stopped directly behind MARSHALL's vehicle. A short time later, while travelling west on West Fond Du Lac Avenue, MARSHALL slowed to a speed well below the posted speed limit forcing a case agent to pass his Escalade. MARSHALL then changed lanes and began to follow directly behind the case agent's vehicle. Several blocks later, MARSHALL pulled into a gas station at 2812 West Fond du Lac Avenue and pulled up to a gas pump. MARSHALL remained stopped at that location until several case agents' vehicles had passed the location. MARSHALL then drove out of the gas station without speaking to anyone or purchasing gas.

78. Case agents resumed surveillance until MARSHALL arrived in the area of a vacant commercial building he owns at 4018 West Center Street, Milwaukee, Wisconsin. MARSHALL did not stop at that location, but drove in a circuitous manner around several of the surrounding streets. Eventually, MARSHALL arrived at a 4-way stop at the same time as a second case agent's vehicle. After driving through the intersection, case agents lost sight of MARSHALL's vehicle. Approximately 15 minutes later, case agents located MARSHALL's Escalade parked at the suspected stash house at 11946 West Mill Road # 25, Milwaukee, Wisconsin. Surveillance was terminated a short time later. Case agents are aware that drug traffickers frequently use countersurveillance techniques to determine if they are being followed. These techniques include following suspected law enforcement vehicles, stopping in public parking lots and observing surrounding vehicles, and driving circuitously through neighborhoods to determine if vehicles are following them. Case agents believe this is the reason for MARSHALL's driving practices that day.

79. On March 18, 2022, the Honorable Nancy Joseph, United States Magistrate Judge in the Eastern District of Wisconsin, signed a warrant authorizing the continued monitoring of location information for Target Cell Phone A for a period of 45 days. That authorization for interception of location information for Target Cell Phone A will expire on May 2, 2022.

80. Since March 18, 2022, case agents have continued to monitor the location of Jonte MARSHALL and Target Cell Phone A. The monitoring of the location of Target Cell Phone A has revealed that MARSHALL continues to frequent locations known to be involved in the drug trafficking and money laundering activities of the MARSHALL DTO. These locations include MARSHALL's current residence in Mequon, Wisconsin; MARSHALL's former residence in West Allis, Wisconsin; the residence of Shomari HOOPER; and the location of a suspected stash house at 11946 West Mill Road # 25, Milwaukee, Wisconsin.

81. Court-authorized positional information for Target Cell Phone A shows that MARSHALL continues to travel the United States and elsewhere. For example, on March 17, 2022, MARSHALL travelled to Miami, Florida before returning to Milwaukee on March 22, 2022. On April 12, 2022, MARSHALL travelled to Atlanta, Georgia before returning to Milwaukee later that same evening. Case agents do not know the purpose of these trips, including the short-term trip to Atlanta.

82. On April 10, 2022, MARSHALL left Milwaukee at approximately 1:46 p.m. and arrived in North Chicago, Illinois, at about 2:31 p.m. MARSHALL left North Chicago at 4:02 p.m. and returned to Milwaukee. Additionally, on April 17, 2022, MARSHALL left Milwaukee at 12:43 p.m. and again travelled to North Chicago, Illinois before returning to Milwaukee at 4:15 p.m. Based on the anonymous tip described above regarding MARSHALL'S drug trafficking

activities with Terrell NEWMAN, case agents believe the short-term travel to Illinois may have been in furtherance of the drug trafficking activities of the MARSHALL DTO.

83. Case agents believed, based on the investigation to date, that Jonte MARSHALL continues to distribute large amounts of fentanyl in the Eastern District of Wisconsin. As detailed above, MARSHALL also continues to utilize Apple platforms, including iCloud, iMessage, and FaceTime to communicate with others regarding the drug trafficking and money laundering activities of the MARSHALL DTO. Case agents believe the receipt of additional information from Apple pursuant to this search warrant will further the investigation and assist with: the identification of additional locations used by the MARSHALL DTO to receive, store, and distribute fentanyl; the identification of other co-conspirators who distribute fentanyl and/or assist in the laundering of drug proceeds for the MARSHALL DTO; and the identification of methods used by DTO members to communicate regarding the drug trafficking and money laundering methods of the MARSHALL DTO.

INFORMATION REGARDING APPLE ID AND iCloud⁸

84. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

⁸ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

85. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio or video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and

presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

86. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

87. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-

party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

88. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

89. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

90. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

91. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging

service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

92. As detailed above, based on a review of phone records, along with physical and electronic surveillance, case agents believe Jonte MARSHALL is using Apple FaceTime and Apple iMessage to communicate with each other and with other DTO members. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

93. Also as detailed above, Jonte MARSHALL has purchased cutting agents used to increase the volume of narcotics prior to distribution, from The Variety Shoppe. Information on the website of The Variety Shoppe indicates that an email will be sent to a customer upon shipment of the package. Therefore, case agents believe the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

94. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs,

documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

95. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

96. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In this investigation, case agents have located bank accounts used by Jonte MARSHALL at at least three different banks. Case agents are aware that each of these banks offer a cellular phone application to allow users to access their accounts. The information connected to an Apple ID may assist in the identification of other bank applications used by MARSHALL. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

97. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

98. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

99. Based on the forgoing, I request that the Court issue the proposed search warrant.

100. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

101. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple IDs : **idtr_black@yahoo.com** (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from July 19, 2021, through May 1, 2022, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from July 19, 2021, through May 1, 2022, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks associated with the account from July 19, 2021, through May 1, 2022;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades associated with the account from July 19, 2021, through May 1, 2022;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps associated with the account from July 19, 2021, through May 1, 2022;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of state and federal controlled substances laws and money laundering laws including Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 1956 and 1957, and other related offenses involving Jonte MARSHALL, Lemonda WARD, Shomari HOOPER, Oscar RAMIREZ-RIVERA, and others since January 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: the sale of illegal drugs and the laundering of proceeds of drug sales.

The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

c. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

d. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____.

_____.

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature